

Amendments to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in this application.

Listing of Claims:

1. (Cancelled)

2. (Currently Amended) A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

~~inserting into a kernel of the operating system a substitute process creation function;~~

creating a first device driver;

loading the first device driver into a kernel of the operating system, wherein the first device driver installs a first process creation wrapper function;

modifying an operating system table consulted by a dispatcher using the first device driver, wherein the modifying an operating system table causes the dispatcher to call the first process creation wrapper function before a process creation function and wherein the first process creation wrapper function and one or more subsequent process creation wrapper functions installed by one or more subsequent device drivers are modifiable so that the one or more subsequent process creation wrapper functions are added and removed serially between the first process creation wrapper function and the process creation function and the one or more subsequent process creation wrapper functions are called by the dispatcher before the process creation function;

intercepting a request for execution of an application executable by a user using the first substitute process creation wrapper function;

communicating information about the request from the first substitute process creation wrapper function to a user-mode application running as a service on the operating system, wherein the communicating information about the request from the first substitute process creation wrapper function to a user-mode application occurs within the operating system;

comparing the information to a list of authorized executables for the user using the user-mode application;

if the information does not match an item on the list, communicating a first message to deny the request from the user-mode application to the first substitute process creation wrapper function; and

if the information does match an item on the list, communicating a second message to permit the request from the user-mode application to the first substitute process creation wrapper function.

3. (Cancelled)

4. (Currently Amended) The method of claim ²/~~3~~, wherein the loading the first device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence.

5. (Cancelled)

6. (Original) The method of claim ²~~3~~, wherein the process creation function provided by the operating system comprises ZwCreateProcess.

7. (Original) The method of claim 2, wherein the information comprises one or more of a user name, an application executable name, and a cryptographic identifier of an application executable.

8. (Original) The method of claim 7, wherein the cryptographic identifier of an application executable comprises a hash created using an MD5 cryptographic algorithm.

9. (Original) The method of claim 2, wherein the list comprises one or more of an application executable name and a cryptographic identifier of an application executable.

10. (Original) The method of claim 2, wherein the comparing the information to a list comprises comparing an application executable name of the information with an application executable name of at least one item from the list.

11. (Original) The method of claim 2, wherein the comparing the information to a list comprises comparing a cryptographic identifier of the information with a cryptographic identifier of at least one item from the list.

12. (Original) The method of claim 2, wherein the communicating information about the request comprises one or more of releasing a semaphore, calling an application program interface function, polling, using a socket, and using a pipe.

13. (Original) The method of claim 2, wherein the communicating a first message to deny the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe.

14. (Original) The method of claim 2, wherein the communicating a second message to permit the request comprises one or more of calling an application program interface function, polling, using a socket, and using a pipe.

15. (Currently Amended) A method for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

~~inserting into a kernel of the operating system a substitute process creation function;~~

creating a first device driver;

loading the first device driver into a kernel of the operating system, wherein the first device driver installs a first process creation wrapper function;

modifying an operating system table consulted by a dispatcher using the first device driver, wherein the modifying an operating system table causes the dispatcher to call the first process creation wrapper function before a process creation function and wherein the first

process creation wrapper function and one or more subsequent process creation wrapper functions installed by one or more subsequent device drivers are modifiable so that the one or more subsequent process creation wrapper functions are added and removed serially between the first process creation wrapper function and the process creation function and the one or more subsequent process creation wrapper functions are called by the dispatcher before the process creation function;

intercepting a request for execution of an application executable by a user using the first substitute process creation wrapper function;

communicating information about the request from the first substitute process creation wrapper function to a user-mode application running as a service on the operating system, wherein the communicating information about the request from the first substitute process creation wrapper function to a user-mode application occurs within the operating system;

prompting the user for authorization to proceed using the user-mode application;

if the authorization is not provided, communicating a first message to deny the request from the user-mode application to the first substitute process creation wrapper function; and

if the authorization is provided, communicating a second message to permit the request from the user-mode application to the first substitute process creation wrapper function.

16. (Original) The method of claim 15, wherein the authorization comprises a password.

17. (Cancelled)

16
18. (Currently Amended) The method of claim 16, wherein the loading the first device driver comprises one of dynamically loading into the kernel and loading into the kernel as part of a boot sequence.

19. (Cancelled)

20. (Currently Amended) A system for preventing process creation of an unauthorized user application executable by an operating system of a computer, comprising:

~~a substitute process creation function, wherein the substitute process creation function is inserted into a kernel of the operating system and intercepts a request for execution of an application executable by a user~~

a first device driver, wherein the first device driver is loaded into a kernel of the operating system;

a first process creation wrapper function, wherein the first device driver installs the first process creation wrapper function in the kernel of the operating system, wherein the first device driver modifies an operating system table consulted by a dispatcher causing the dispatcher to call the first process creation wrapper function before a process creation function, and wherein the first process creation wrapper function and one or more subsequent process creation wrapper functions installed by one or more subsequent device drivers are modifiable so that the one or more subsequent process creation wrapper functions are added and removed serially between the

first process creation wrapper function and the process creation function and the one or more subsequent process creation wrapper functions are called by the dispatcher before the process creation function; and

a user-mode application running as a service on the operating system, wherein the communicating information about the request from the first substitute process creation wrapper function to a user-mode application occurs within the operating system and; wherein the a user-mode application receives information about the request from the first substitute process creation wrapper function, compares the information to a list of authorized executables for the user, communicates a first message to deny the request to the first substitute process creation wrapper function, if the information does not match an item on the list, and communicates a second message to permit the request to the first substitute process creation wrapper function, if the information does match an item on the list.

21. (Original) The system of claim 20, further comprising an administrative server, wherein the administrative server is in communication with the user-mode application, and wherein the user-mode application downloads the list from the administrative server.